Amendments to the Claims

Claims 1-20 and 22-24 are pending. Claims 1-17, 20, and 22-24 are being amended. Claim 21 has been canceled. The following listing of claims replaces all previous versions of the claims in the application.

Listing of Claims

1. (currently amended) A method for using identity-based encryption (IBE) to securely convey messages in a system in which senders communicate with recipients over a communications network ~~from a sender to a recipient~~, wherein the recipients ~~has~~ each have an associated IBE public key and an associated IBE private key for use in IBE encryption and decryption, wherein the system includes a plurality of IBE private key generators each of which generates a plurality of associated IBE private keys for a plurality of associated recipients to use in decrypting messages encrypted with their respective IBE public keys, wherein each IBE private key generator generates different IBE public parameter information to be used in encrypting messages for its associated recipients, wherein the different IBE public parameter information generated by each IBE public key generator is maintained by a different respective IBE public parameter host, and wherein each IBE

public parameter host has a different service name ~~wherein the sender uses the IBE public key of the recipient and IBE public parameter information associated with the recipient to encrypt messages for the recipient, wherein the IBE public parameter information is maintained on an IBE public parameter information host that provides the IBE public parameter information over the communications network, and wherein the host has a service name~~ that is used to communicate with ~~the~~ that host over the network, the method comprising:

at ~~the~~ a sender who desires to send an encrypted message to a given recipient who is associated with a given one of the plurality of IBE public parameter information hosts, using a service name generation rule to determine which of the IBE public parameter hosts should be contacted to obtain the IBE public parameter information that is associated with the given recipient and that is to be used in encrypting the message to the given recipient, wherein using the service name generation rule comprises using the service name generation rule to generate the service name of the IBE public parameter information host that is associated with the given recipient based on the IBE public key of the recipient;

using the service name to obtain the IBE public parameter information associated with the given recipient for the sender from the IBE public parameter host that is associated

with the given recipient over the network; and

at the sender, using the IBE public parameter information obtained from the IBE public parameter host and the IBE public key of the recipient to encrypt a message for the recipient.

2. (currently amended) The method defined in claim 1 further comprising:

at the sender, using the service name generated with the service generation rule and the IBE public key to provide the IBE public parameter host that is associated with the given recipient with a request that the host provide the IBE public parameter information to the sender; and

with the IBE public parameter host that is associated with the given recipient, providing the IBE public parameter information to the sender in response to the request for the IBE public parameter information from the sender.

3. (currently amended) The method defined in claim 2 further comprising:

at the sender, sending the request to the host ~~server~~ that is associated with the given recipient as an email message.

4. (currently amended) The method defined in claim 1 ~~wherein an IBE private key generator is connected to the network, the method~~ further comprising electronically conveying the IBE public parameter information maintained at each IBE public parameter host from the IBE private key generator ~~to the~~ that is associated with that IBE public parameter host to that IBE public parameter host over the network.

5. (currently amended) The method defined in claim 1 wherein the given recipient has a message address, the method further comprising:

at the sender, using the service name generation rule to generate the service name of the IBE public parameter information host associated with the given recipient by prepending a string to at least a portion of the message address.

6. (currently amended) The method defined in claim 1 wherein the given recipient has an email address having a domain name portion, the method further comprising:

at the sender, using the service name generation rule to generate the service name of the IBE public parameter information host associated with the given recipient by prepending a string to the domain name portion of the email

address.

7. (currently amended) The method defined in claim 1 wherein ~~the~~ each IBE public parameter information host has an identity, the method further comprising:

at the sender, verifying the identity of the IBE public parameter information host from which the IBE public parameter information for the given recipient is obtained.

8. (currently amended) The method defined in claim 7 wherein verifying the identity of the IBE public parameter information host associated with the given recipient comprises:

at the sender, comparing service name information received from the IBE public parameter information host associated with the given recipient by the sender to the service name generated with the service name generation rule to determine whether there is a match.

9. (currently amended) The method defined in claim 7 wherein the IBE public key of the given recipient includes a message address having a domain name portion and wherein verifying the identity of the IBE public parameter information host associated with the given recipient comprises:

at the sender, comparing identity information

received from the IBE public parameter information host associated with the given recipient by the sender to the domain name portion of the message address to determine whether the identity information matches the domain name portion.

10. (currently amended) The method defined in claim 7 wherein a certificate authority provides a certificate that contains the service name of the IBE public parameter information host associated with the given recipient and wherein verifying the identity of the IBE public parameter information host associated with the given recipient comprises:

providing the certificate that contains the service name of the IBE public parameter information host associated with the given recipient to the sender so that the sender can compare signed service name information in the certificate to the service name of the host that was generated by the service name generation rule to determine whether there is a match.

11. (currently amended) The method defined in claim 1 further comprising, with the IBE public parameter information host associated with the given recipient, providing the sender with identity information signed by a certificate authority.

12. (currently amended) The method defined in claim 1 further comprising, with the IBE public parameter information host associated with the given recipient, providing the sender with the IBE public parameter information signed by a certificate authority.

13. (currently amended) The method defined in claim 1 wherein providing the IBE public parameter information associated with the given recipient to the sender comprises providing the IBE public parameter information associated with the given recipient to the sender over a secure communications link.

14. (currently amended) The method defined in claim 1 wherein providing the IBE public parameter information associated with the given recipient to the sender comprises providing the IBE public parameter information associated with the given recipient to the sender over an insecure communications link.

15. (currently amended) The method defined in claim 14 wherein providing the IBE public parameter information associated with the given recipient to the sender over the insecure link comprises using the IBE public parameter

information host associated with the given recipient to encrypt the IBE public parameter information associated with the given recipient in a message format prior to sending the IBE public parameter information associated with the given recipient to the sender in the message format over the insecure link.

16. (currently amended) The method defined in claim 1 wherein the message is an email message and wherein the IBE public key of the given recipient comprises an email address, the method further comprising:

at the sender, using the email address of the given recipient to send the email message to the given recipient over the communications network.

17. (currently amended) The method defined in claim 1 wherein the message is an instant message and wherein the IBE public key of the given recipient comprises an instant message address, the method further comprising:

at the sender, using the instant message address of the given recipient to send the instant message to the given recipient over the communications network.

18. (original) The method defined in claim 1 further comprising providing the sender with the service name generation

rule in a plug-in module.

19. (original) The method defined in claim 1 further comprising providing the sender with the service name generation rule as part of an email program.

20. (currently amended) The method defined in claim 1 wherein the service name comprises a domain name, the method further comprising:

at the sender, using the domain name to establish a secure sockets layer communications link with the IBE public parameter information host associated with the given recipient over the Internet.

21. (canceled)

22. (currently amended) The method defined in claim 1 wherein the given recipient comprises a router having an associated IP addresses and wherein the host has an associated IP address, the method further comprising:

at the sender, using the service name generation rule to generate the service name from the given recipient's IP address by changing at least one variable byte in the recipient's IP address to create the IP address of the host.

23. (currently amended) The method defined in claim 1 wherein the IBE public key of the given recipient contains at least one geographical region attribute, the method further comprising using the service name generation rule to generate the service name by basing the service name at least partially on the geographical region attribute.

24. (currently amended) The method defined in claim 1 ~~wherein there are a plurality of IBE public parameter information hosts, each of which maintains different IBE public parameter information and each of which has a different associated service name, and~~ wherein the given recipient has an email address having a domain name portion, the method further comprising:

at the sender, using the service name generation rule to generate the service name ~~that is associated with a particular one of the plurality~~ of the IBE public parameter information host~~s~~ associated with the given recipient by prepending a string to the domain name portion of the given recipient's email address and using that service name to obtain the IBE public parameter information from ~~that particular one of the plurality of~~ the IBE public parameter information host~~s~~ associated with the given recipient over the communications

network.